

М. П. Мучин¹, П. В. Мучин²✉

Обзор информационно-коммуникационных технологий, повышающих уровень техносферной безопасности

¹Сибирский государственный университет телекоммуникаций и информатики,
г. Новосибирск, Российская Федерация

²Сибирский государственный университет геосистем и технологий, г. Новосибирск,
Российская Федерация
e-mail: p.v.muchin@snga.ru

Аннотация. В работе проведен обзор информационно-коммуникационных технологий (ИКТ), направленных на повышение уровня техносферной безопасности. Рассмотрены и систематизированы ключевые категории ИКТ: системы автоматизации (SCADA/АСУТП), промышленные сети IoT/IIoT, телекоммуникационные инфраструктуры (4G/5G, LPWAN), геоинформационные системы, беспилотные летательные аппараты, цифровые двойники и средства кибербезопасности. Особое внимание уделено роли искусственного интеллекта (машинного обучения, глубоких нейросетей, компьютерного зрения) в обнаружении аномалий, прогнозировании аварий и автоматизации процессов реагирования. Отдельно рассмотрен потенциал ИКТ в электронной промышленности России. Выявлены риски внедрения (киберугрозы, устаревшее оборудование, дефицит кадров) и даны практические рекомендации.

Ключевые слова: информационно-коммуникационные технологии, техносферная безопасность, искусственный интеллект (ИИ), 5G, IoT, цифровые двойники, предиктивное обслуживание, кибербезопасность, электронная промышленность

M. P. Muchin¹, P. V. Muchin²✉

A review of information and communication technologies that improve the level of technosphere safety

¹Siberian state university of Telecommunications and Informatics, Novosibirsk, Russian Federation

²Siberian state university of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: p.v.muchin@snga.ru

Annotation. This paper provides an overview of information and communications technologies (ICT) aimed at improving technosphere security. Key ICT categories are examined and systematized: automation systems (SCADA/APCS), industrial IoT/IIoT networks, telecommunications infrastructures (4G/5G, LPWAN), geographic information systems, unmanned aerial vehicles, digital twins, and cybersecurity tools. Particular attention is paid to the role of artificial intelligence (machine learning, deep neural networks, computer vision) in anomaly detection, accident prediction, and automated response processes. The potential of ICT in the Russian electronics industry is separately considered. Implementation risks (cyber threats, obsolete equipment, personnel shortages) are identified, and practical recommendations are provided.

Key words: information and communications technology, technosphere security, artificial intelligence (AI), 5G, IoT, digital twins, predictive maintenance, cybersecurity, electronics industry

Введение

Раскрытие заявленной темы требует введения ряда определений. Ключевыми понятиями являются техносфера, производственная деятельность,

безопасность и информационно-коммуникационные технологии.

Очевидно, что техносфера является частью глобальной экосферы и содержит совокупность искусственных технических сооружений, предметов и пр., которые производятся и используются (эксплуатируются) человеком.

В соответствии с Трудовым кодексом Российской Федерации производственную деятельность необходимо рассматривать как «совокупность действий работников с применением средств труда, необходимых для превращения ресурсов в готовую продукцию, включающих в себя производство и переработку различных видов сырья, строительство, оказание различных видов услуг».

Производственная деятельность интегрируется в систему техносферы и порождает понятие – производственная безопасность (безопасные условия труда) — условия, при которых воздействие на работающих вредных и (или) опасных производственных факторов исключено либо уровни воздействия таких факторов не превышают установленных нормативов.

В свою очередь производственная безопасность интегрирует (включает) такие понятия, как охрана труда, а также пожарная, промышленная, транспортная, экологическая, радиационная, химическая, биологическая, технологическая и другие виды безопасности [1, 2].

В современных условиях жизни человеческого общества, особенно в области трудовых отношений, все большее значение приобретают информационно-коммуникационные технологии, в том числе в обеспечении приемлемого уровня безопасности.

С одной стороны, ИКТ расширяют возможности мониторинга и анализа опасных процессов (например, с помощью сенсоров и видеокамер), с другой — создают новые уязвимости (цифровые сбои и кибератаки могут привести к физическим авариям). В результате промышленное производство сталкивается с необходимостью интегрировать средства цифрового контроля и управления при одновременном соблюдении жестких стандартов безопасности.

В настоящее время уже невозможно представить современный мир без телекоммуникационных технологий, которые стирают границы между людьми, городами и государствами, поскольку обеспечивается уровень общения практически «без расстояния». Общее определение информационно-коммуникационным технологиям возможно, как «совокупность различных технических средств, способов, методов и устройств, позволяющих решать задачи по сбору, обработке, хранению и передаче информации, чаще в электронном (цифровом) виде».

Для экономики России, в условиях санкционных ограничений, развитие информационно-коммуникационных технологий становится действенным инструментом повышения эффективности производственной деятельности и, что особенно важно, техносферной безопасности [2].

Методы и материалы

В настоящее время научные и технические основы создания и развития ИКТ хорошо проработаны и, соответственно, в настоящей работе не ставится цель решать проблемы развития или совершенствования ИКТ. В нашей работе будет

сделана попытка систематизации ключевых категорий информационно-коммуникационных технологий и показать их практическое влияние на техносферную безопасность [2].

Информационно-коммуникационные технологии влияют на техносферную безопасность через несколько функциональных категорий. Системы управления и контроля (SCADA/АСУТП) осуществляют диспетчеризацию технологических процессов: собирают телеметрию и выдают команды исполнительным механизмам. Эти системы непосредственно управляют физическими объектами, поэтому их сбои или взломы приводят к аварийным ситуациям. Многие протоколы автоматизации изначально не предусматривали механизмы аутентификации и шифрования, что требует применения современных мер безопасности.

Для передачи информации (данных) в ИКТ-системах широко применяются сетевые и коммуникационные технологии. При этом широко используются сотовые сети формата скорости передачи 4G и 5G.

Стремительное развитие 5G-технологий обеспечивает высокую скорость передачи информации и, соответственно, достичь сверхнизкой задержки способствуя повышению надежности системы.

Сбор информации о состоянии применяемого оборудования, о действиях работающего персонала и качестве рабочей среды (рабочей зоны, рабочих мест) достигается сенсорами и IoT-устройствами [2].

В обеспечении техносферной безопасности широко применяются возможности геоинформационных систем (ГИС). Использование картматериала (планов, снимков) обеспечивает возможности пространственного анализа и визуализацию рисков. Научно-исследовательскими организациями, вузами и структурами МЧС России достаточно давно ГИС-технологии применяются для моделирования зон распространения химических выбросов с учетом розы ветров, формирование и оценка лавиноопасных участков и др.

Беспилотные летательные аппараты (БПЛА) используются для мобильной разведки опасных территорий. Дроны позволяют быстро обследовать зоны пожаров, наводнений и техногенных аварий. На промышленных объектах БПЛА проводят визуальный осмотр конструкций, патрулирование периметра и мониторинг тепловизором, сокращая время осмотра и повышая безопасность обследований без риска для человека.

Цифровые двойники представляют собой виртуальные модели реальных предприятий и систем. Данный инструмент позволяет симулировать работу объекта в реальном времени и отрабатывать сценарии аварий. Виртуальное моделирование аварийных ситуаций дает возможность отработки реакций служб до реального инцидента и используется для подготовки персонала.

Далее покажем отдельные примеры успешного применения телекоммуникационных систем, в том числе с возможностью повысить безопасность работников, как в мировой, так и в российской практике.

Положительные примеры использования 5G и IoT широко представлены как в мировой, так и в российской практике. Немецкий автопроизводитель «Audi» в партнерстве с компанией «Ericsson» активно использует технологию 5G

URLLC для управления роботами на сборочных линиях. Задержка сигнала менее 5 мс позволяет мгновенно останавливать оборудование при приближении человека к опасной зоне, что существенно повышает уровень безопасности.

Примеры продуктивного использования ИИ в сочетании с системой «5G-периферийные вычисления» показывает компания «Huawei» (Китай). Контроль качества приближается к 100 % [2, 3].

Еще один положительный пример показывает фирма «Siemens», где внеплановые остановки оборудования снизились на разных производственных участках на 20–50 % благодаря успешному применению технологии IoT при реализации предиктивного обслуживания.

В последние годы возрастает роль искусственного интеллекта в обеспечении техносферной безопасности. Применение нейронных сетей повышает способность успешного обнаружения сложных аномалий и, соответственно, предсказывать возможные остановки, аварии и др.

Алгоритмы глубокого обучения анализируют видеопоток с камер безопасности: они автоматически фиксируют нарушение техники безопасности (отсутствие каски у рабочего, выход за огражденную опасную зону). Как показали примеры из металлургии, система «ИИ-фотоанализ» продемонстрировала выявление 95–98 % нарушений применений средств индивидуальной защиты (СИЗ) и сократила количество несчастных случаев почти в восемь раз.

На Магнитогорском металлургическом комбинате система машинного зрения с RFID-метками на касках контролирует использование СИЗ. На Быстринском ГОКе («Норникель») нейронная сеть распознает отсутствие средств защиты. Госкорпорация «Росатом» с 2019 г. применяет умную видеоаналитику на Кольской АЭС: анализ более 2 млн параметров снижает расходы на обслуживание на 30 % и брак до 0,9 % [2, 4].

Ранее авторами проводилось сравнительное тестирование нейронных сетей в образовании при подготовке специалистов техносферной безопасности (ChatGPT-4, ChatGPT 4o, DeepSeek-R1, Grok 3, o3-mini-high). Результаты показали ограничения бесплатных версий (средний показатель правильности ответов 25–74 %), в том числе генерацию несуществующих нормативных правовых актов. Платные версии (у нас это o3-mini-high) демонстрируют существенно более высокий потенциал. Это подтверждает, что в системе образования ИИ может помогать в решении расчетных задач, однако для реального производства требуются специализированные модели ИИ [5, 6].

Отдельное внимание необходимо уделить возможностям ИКТ в электронной промышленности Российской Федерации — отрасли, где трудится порядка 300 тыс. человек и выполняющая ключевую роль в разработке оборудования и программного обеспечения для реализации современных технологий безопасности.

В 2020 г. Правительством России утверждена «Стратегия развития электронной промышленности до 2030 года». Отрасль реализует задачи по разработке и производству не только электронного оборудования, но и встраиваемого программного обеспечения. Правительством поставлены прямые задачи:

разработать и внедрить автоматизированную систему управления отраслью и систему управления рисками развития отрасли [7].

Очевидно, что реализация поставленных задач невозможна без развития и внедрения современных информационных технологий (ИТ). В электронной промышленности часто требуется оценка химических рисков, риска поражения электрическим током и др., особенно для разработки и использования микроэлектроники. Современные ИТ (MES, ERP, ACS, оптическое и лазерное сканирование, IoT и ИИ) позволяют автоматизировать контроль качества, сокращать ошибки человеческого фактора и внедрять симуляторы для обучения. Пример — системы машинного зрения на заводах «Foxconn» с Google Cloud Visual Inspection AI (точность выявления дефектов до 99 %). В России такие решения интегрируются в рамках государственной программы, обеспечивая не только экономическую эффективность, но и защиту работников через предиктивный мониторинг и виртуальное моделирование чрезвычайных ситуаций.

Помимо указанных выше технологий, значительный вклад в повышение техносферной безопасности вносит и метод 3D-анимации.

Ранее авторами были показаны возможности 3D-анимации в 3ds Max для моделирования пожароопасных ситуаций (срабатывание фотоэлектрического датчика дыма в гостиничном номере). Такие ролики повышают культуру безопасности, популяризируют датчики и включаются в сайты организаций для роста конкурентоспособности. Аналогичные анимации используются в обучении и лабораторных работах [2, 8, 9].

Для эффективной работы всех перечисленных технологий необходима чётко выстроенная архитектура систем, надёжные протоколы передачи данных и соблюдение международных и национальных стандартов.

Ключевой стандарт — IEC 62443 («Security for industrial automation and control systems»): сегментация сети, аутентификация, управление уязвимостями. В России он принят как «ГОСТ Р МЭК» и обязателен для объектов критической информационной инфраструктуры (КИИ). Дополняется ISO/IEC 27019 для энергетики и требованиями Федеральной службы по техническому и экспортному контролю (ФСТЭК России) [10].

Внедрение ИКТ сопряжено с рисками. В качестве примера отметим несколько основных:

- киберугрозы;
- ошибки ИИ;
- этика и приватность;
- надёжность связей.

Среди основных проблем отметим: киберугрозы (37 % атак через сетевые уязвимости), эксплуатацию устаревшего оборудования (адаптация через SDN), нехватку квалифицированных кадров (прогноз - к 2030 г. дефицит достигнет 85 миллионов специалистов), наличие помех в беспроводных сетях.

Результаты

Выполненный обзор подтверждает, что интеграция ИКТ существенно повышает техносферную безопасность. Применение технологий SCADA/АСУТП, IoT, современных сетей и ИИ обеспечивает переход от реактивного к проактивному управлению рисками. Примеры из энергетики и промышленности демонстрируют реальное сокращение аварийности. 3D-анимация и цифровые двойники формируют новую культуру безопасности. Автоматизированные рабочие места специалистов по охране труда, «Единая общероссийская справочно-информационная система по охране труда» (ЕИСОТ), порталы тестирования по промышленной безопасности — все эти технологии построены на использовании ИКТ [2, 8-10].

Заключение

В процессе выполненного исследования для нас становится очевидным, что информационно-коммуникационные технологии являются фундаментом для перехода экономики к цифровой эпохе. Для нашего государства, находящегося в условиях санкционного давления, развитие собственных телекоммуникационных технологий становится вопросом национальной безопасности и экономической устойчивости.

Стремительное развитие информационно-коммуникационных технологий требует постоянного, пристального внимания государственных органов власти к обновлению и совершенствованию нормативно-правовой базы, регулирующей как процесс обучения, так и производственную составляющую, в том числе — финансовое обеспечение исследований.

Практика показывает, что уже на современном этапе, практически каждый объект экономики нашего государства, имеет возможность достаточно эффективно применять очень многие информационные технологии, в том числе способствующие повышению уровня техносферной безопасности. Эта задача достаточно актуальная, так как это позволяет сохранить здоровье и жизнь человека (работника), который является, особенно для нашего государства, самым важным и дорогим ресурсом, в том числе в экономике.

Очевидно, что развитие ИКТ и искусственного интеллекта, в настоящее время, реализуется с нарастающими темпами. Учитывая глобальную задачу по цифровизацию Российской экономики и повышения ее конкурентоспособности, обостряется задача по защите работников. Решение поставленных задач требует разумного сочетания потенциала и ресурсов научного и преподавательского сообществ при активной участии государственных органов власти.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон от 29.12.2012 № 273-ФЗ (ред. от 29.12.2025) «Об образовании в Российской Федерации». [Электронный ресурс] — Режим доступа: <https://docs.cntd.ru/document/902389617?ysclid=mmm9fnwbva208224625>.
2. Мучин П. В., Мучин М. П. Информационно-коммуникационные технологии в организации производственной деятельности в аспекте обеспечения безопасности // Материалы XXI

Международного научного конгресса Интерэкспо ГЕО-Сибирь. – Новосибирск : СГУГиТ, 2025. - Том 3. - С. 66-73.

3. 5G для комбината. [Электронный ресурс] - Режим доступа: <https://rspectr.com/articles/5g-dlya-kombinata/>.

4. НЛМК: искусственный интеллект на службе у сталеваров. [Электронный ресурс] - Режим доступа: <https://www.osp.ru/cio/2018/01/13053828/>.

5. Мучин П. В., Мучин М. П. Экспертное тестирование возможностей нейронной сети ChatGPT-4 в русскоязычном сегменте информационного поля при решении отдельных проблем техносферной безопасности // Материалы XIX Международного научного конгресса Интерэкспо ГЕО-Сибирь. – Новосибирск : СГУГиТ, 2023. - Том 3. - С. 268-275.

6. Мучин П. В., Мучин М. П. Искусственный интеллект в образовании: сравнительное тестирование ChatGPT 4o, DeepSeek-R1 и Grok 3 по направлению подготовки «Техносферная безопасность» // Материалы Национальной научно-методической конференции с международным участием «Актуальные вопросы образования. Современное высшее инженерное образование: содержание, качество, технологии, кадры». – Новосибирск : СГУГиТ, 2025. Часть 2. - С. 132-137.

7. «Стратегия развития электронной промышленности Российской Федерации на период до 2030 года», утверждена распоряжением Правительства Российской Федерации от 17.01.2020 № 20-р. [Электронный ресурс] - Режим доступа: <http://static.government.ru/media/files/1QkfNDghANiBUNBbXaFBM69Jxd48ePeY.pdf>.

8. Мучин М. П., Тимофеев Н. А., Мучин П. В. Исследование возможностей применения метода 3D анимации для решения прикладных задач, связанных с повышением уровня производственной безопасности // Материалы XVII Международного научного конгресса Интерэкспо ГЕО-Сибирь. – Новосибирск : СГУГиТ, 2021. - Т. 7, №. 2. - С. 127-134.

9. Тимофеев Н. А., Мучин М. П., Сат Т. А. Возможности реализации трехмерного моделирования для разработки элементов дополненной реальности в интерактивных туристических картах // Материалы XIX Международного научного конгресса Интерэкспо ГЕО-Сибирь. – Новосибирск : СГУГиТ, 2025. - Том 7, № 2 - С. 82-88.

10. «ГОСТ Р МЭК 62443-3-3-2016 Требования к системной безопасности и уровни безопасности». [Электронный ресурс] - Режим доступа: <https://docs.cntd.ru/document/1200135801?ysclid=mmxiljwzz9969920775>.

© М. П. Мучин, П. В. Мучин, 2026